МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧЕРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
(БГТУ им. В.Г.Шухова)

УТВЕРЖДАЮ
Директор института ЭИТУС
А.В. Белоусов
«28» 05 2021 г.

РАБОЧАЯ ПРОГРАММА
дисциплины

Информационная безопасность

Направление подготовки

18.05.02 Химическая технология материалов современной энергетики

Направленность программы

Ядерная и радиационная безопасность на объектах использования ядерной энергии

Квалификация

Инженер

Форма обучений

очная

Институт: Энергетики, информационных технологий и управляющих систем

Кафедра: Информационных технологий

Белгород – 2021

Образовательная программа составлена на основании с требованиями:

- Федерального государственного образовательного стандарта высшего образовани - специалитет по специальности 18.05.02 Химическая технология материало современной энергетики, утвержденного приказом Минобрнауки России с 07.08.2020 г. № 913;

- Учебного плана, утвержденного ученым советом БГТУ им. Шухова в 2021 г.

Составитель (составители): _____ (Е.П. Коломыцева)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа обсуждена на заседании кафедры

«30» 04 2021 г., протокол № 6

и.о. заведующий кафедрой: к.т.н., доцент _____ (Д.Н. Старченко)
(ученая степень и звание, подпись) (инициалы, фамилия)

Рабочая программа согласована с выпускающей кафедрой теоретической и прикладной химии
Зав. кафедрой: доктор техн.наук, профессор _____(В.И. Павленко)

«13» мая 2021г., протокол № 9

Рабочая программа одобрена методической комиссией института

«20» 05 2021 г., протокол № 9

Председатель к.т.н., доцент _____(А.Н. Семернин)
(ученая степень и звание, подпись) (инициалы, фамилия)

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Категория (группа) компетенций	Код и наименования компетенции	Код и наименование индикатора достижения компетенции	Наименование показателя оценивания
Общепрофессиональные компетенции	ОПК-6. Способен использовать информацию, полученную при осуществлении своей профессиональной деятельности, с учетом основных требований информационной безопасности в том числе защиты государственной тайны	ОПК-6.1 Использует информацию, полученную при осуществлении профессиональной деятельности с учетомтребований информационной безопасности	**Знания**: технические и программныесредств реализации информационных процессов; методы и процессы сбора, передачи, обработки и накопления информации; **Умения**: использовать возможности вычислительной техники и программного обеспечения; выполнять обобщение и систематизацию технических данных; осуществлять выбор наиболее эффективных методов, способов и средств получения, хранения и переработки информации в зависимости от конкретных целей и задачпрофессиональной деятельности; **Навыки:** использовать возможности глобальных компьютерных сетей;
		ОПК-6.2 Применяет методы информационной безопасности при подготовке проектной и технической документации в сфере профессиональной деятельности	**Знания**: теоретические основы изучаемых алгоритмов шифрования, формы защиты информации в сети Интернет, требования к защите информации, критерии оценки угроз. **Умения:** проводить анализ необходимой информации, технических данных, показателей ирезультатов работы; **Навыки:** работать с различными источниками информации, используя разные формы защиты информации, выявлять программы – шпионы, «вирусы».

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Компетенция ОПК-6. Способен использовать информацию, полученную при осуществлении своей профессиональной деятельности, с учетом основных требований информационной безопасности в том числе защиты государственной тайны.

Данная компетенция формируется следующими дисциплинами.

Стадия	Наименование дисциплины
1	Информационная безопасность
2	Выполнение, подготовка к процедуре защиты и защита Выпускной квалификационной работы

3. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4 зач. единиц, 144 часа.

Форма промежуточной аттестации: Зачет

Вид учебной работы	Всего часов	Семестр № 5
Общая трудоемкость дисциплины, час	144	144
Контактная работа (аудиторные занятия), в т.ч.:	53	53
лекции	17	17
лабораторные	-	-
практические	34	34
групповые консультации в период теоретического обучения и промежуточной аттестации	2	2
Самостоятельная работа студентов, включая индивидуальные и групповые консультации, в том числе:	91	91
Курсовой проект	-	-
Курсовая работа	-	-
Расчетно-графическое задание	-	-
Индивидуальное домашнее задание	-	-
Самостоятельная работа на подготовку к аудиторным занятиям (лекции, практические занятия, лабораторные занятия)	91	91
Форма промежуточной аттестации (зачет, экзамен)	-	-

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Наименование тем, их содержание и объем

Курс 3 Семестр 5

№ п/п	Наименование раздела (краткое содержание)	Объем на тематический раздел по видам учебной нагрузки, час			
		Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа
1.	**Раздел 1.Основные аспекты информационной безопасности**				
	Понятие информационной безопасности. Основные категории информационной безопасности. Законодательные аспекты информационной безопасности. Анализ наиболее распространенных угроз и методов проникновения в информационные системы. Программное обеспечение, применяемое для проникновения в информационные системы и методы нейтрализации его воздействия.	1			1
2.	**Раздел 2. Криптографические средства защиты информации**				
	Основные понятия криптографии, терминология. Классификация криптоалгоритмов. Основные виды криптоаналитических атак. Законодательство РФ в области разработки и применения систем, содержащих элементы криптозащиты. Потоковые и блочные шифры. Принципы построения блочных шифров. Конструкции Фейстеля. Режимы работы блочных шифров. Криптоалгоритмы AES, ГОСТ 28147-89 и ГОСТ Р 34.12-2015.Основные принципы шифрования с открытым ключом. Области применения криптосистем с открытым ключом. Криптоалгоритм RSA. Управление ключами. АлгоритмДиффи-Хеллмана-Меркла.	6		22	28
3.	**Раздел 3. Стандарты информационной безопасности**				
	Основные понятия, вводимые стандартами и спецификациями. Руководящие документы Гостехкомиссии РФ. Нормативные документы ФСТЭК. Обзор наиболее значимых отечественных стандартов в области информационной безопасности: ИСО/МЭК 15408, серия стандартов ИСО/МЭК 27000.	1			2
4.	**Раздел 4. Электронная подпись и аутентификация**				
	Назначение функций хэширования и предъявляемые к ним требования. Обзор известных алгоритмов хэширования: MD5, SHA-1, 2, 3, ГОСТ Р 34.11-94, 2012.Требования к электронным подписям. Основные положения закона 63-ФЗ «Об электронной подписи». Характеристики алгоритмов	4		6	10

	создания и верификации электронных подписей: DSA,ECDSA, ГОСТ Р 34.10-94, 2001, 2012. Протоколы односторонней и двусторонней аутентификации на основе симметричного и асимметричного шифрования. Основные положения стандарта X.509. Структура сертификата открытого ключа, форматы хранения. Отзыв сертификатов. Общая схема аутентификации с использованием сертификатов X.509. Инфраструктуры открытых ключей.				
5.	**Раздел 5. Защита распределенных систем и корпоративных сетей**				
	Особенности протоколов защищенного обмена данными сетевого и транспортного уровня и их место в стеке протоколов TCP/IP. Обзор защищенных протоколов: IPSec, SSL, TLS. Атакуемые сетевые компоненты информационных систем. Классификация нарушителей сетевой безопасности информационных систем. Управление доступом. Методика обнаружения нарушителей. Протоколирование и аудит. Классификация вредоносных программ. Антивирусная защита. Основные характеристики и типы брандмауэров и систем обнаружения и предотвращения вторжений.	2		6	8
6.	**Раздел 6. Системы защиты электронной почты**				
	Назначение и принцип работы систем PGPи S/MIME.	2			3
7.	**Раздел 7. Организационное обеспечение информационной безопасности**				
	Административный уровень информационной безопасности. Формирование политики безопасности. Управление рисками. Процедурный уровень информационной безопасности. Основные меры поддержания работоспособности информационной системы.	1			1
	ВСЕГО	17		34	53

4.2. Содержание практических (семинарских) занятий

№ п/п	Наименование раздела дисциплины	Тема лабораторного занятия	К- во часов	К-во часов СРС
семестр № 8				
1	Криптографические средства защиты информации	Потоковое шифрование данных	4	4
2		Алгоритм блочного шифрования данных ГОСТ 28147-89	6	6
3		Симметричное шифрование данных с использованием криптографических интерфейсов MicrosoftCryptoAPI и Cryptography API: NextGeneration	6	6
4		Симметричное и асимметричное шифрование данных средствами криптографического пакета OpenSSL	6	6

5	Электронная подпись и аутентификация	Создание криптографических сообщений с использованием интерфейса MicrosoftCryptoAPI и цифровых сертификатов X.509	6	6
6	Защита распределенных систем и корпоративных сетей	Реализация защищенной передачи данных по протоколу TLS средствами криптографического пакета OpenSSL	6	6
		ИТОГО:	34	34
			ВСЕГО:	68

4.3. Содержание лабораторных занятий

Лабораторные занятия при изучении дисциплины не предусмотрены учебным планом.

4.4. Содержание курсового проекта/работы

Курсовые работы и курсовые проекты при изучении дисциплины не предусмотрены учебным планом.

4.5. Содержание расчетно-графического задания, индивидуальных домашних заданий

Индивидуальные домашние задания при изучении дисциплины не предусмотрены учебным планом.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1. Реализация компетенции

Компетенция ОПК-6. Способен использовать информацию, полученную при осуществлении своей профессиональной деятельности, с учетом основных требований информационной безопасности в том числе защиты государственной тайны.

Наименование индикатора (показателя оценивания)	Используемые средства оценивания
ОПК-6.1 Использует информацию, полученную при осуществлении профессиональной деятельности с учетом требований информационной безопасности	Зачет.
ОПК-6.2 Применяет методы информационной безопасности при подготовке проектной и технической документации в сфере профессиональной деятельности	Зачет.

5.2. Типовые контрольные задания для промежуточной аттестации

5.2.1. Перечень контрольных вопросов (типовых заданий) для зачета

№ п/п	Наименование раздела дисциплины	Содержание вопросов (типовых заданий)
1	Основные аспекты информационной безопасности (ОПК-6)	Понятие информационной безопасности. Основные типы угроз информационной безопасности
		Законодательные аспекты информационной безопасности.
2	Криптографические средства защиты информации (ОПК-6)	Базовые понятия криптографии. Основные задачи, решаемые с помощью криптографии. Понятия криптоалгоритма и ключа
		Криптоанализ. Понятие стойкости алгоритма. Основные разновидности криптоаналитических атак
		Классификация алгоритмов классической криптографии. Одноразовые блокноты. Классификация компьютерных криптоалгоритмов.
		Принципы построения блочных шифров. Сеть Фейстеля
		Основные режимы работы блочных шифров
		Криптоалгоритм ГОСТ 28147-89. Структура раунда. Базовые циклы зашифрования и расшифрования. Режимы шифрования, определенные стандартом
		КриптоалгоритмAES. Характеристики алгоритма и его структура
		Криптосистемы с открытым ключом. Принципы построения и отличия от симметричных криптосистем. Алгоритм с открытым ключом RSA
		Управление ключами в симметричных и асимметричных криптосистемах. Генерация ключей. Распределение ключей для симметричных криптосистем
		Обмен сеансовыми ключами средствами симметричной криптографии и криптографии с открытым ключом. Способы хранения ключей. Время жизни ключей
		Алгоритм обмена ключами Диффи-Хеллмана-Меркла.
		Потоковые шифры A5 и RC4
3	Стандарты информационной Безопасности (ОПК-6)	Стандарты информационной безопасности РФ
4	Электронная подпись и аутентификация (ОПК-6)	Однонаправленные хэш-функции. Назначение. Основные требования, предъявляемые к хэш-функциям. Коллизии и их использование в процессе подделки сообщений
		Характеристики и общие принципы построения алгоритмов хэшированияMD5, SHA-1, 2, 3, ГОСТ Р 34.11-94, 2012
		Коды проверки подлинности сообщений (MAC)
		Электронная подпись (ЭП). Назначение электронной подписи, ее виды. Требования к ЭП. Общие принципы создания ЭП. Стандарты ЭП РФ и США
		Протоколы односторонней и двухсторонней аутентификации
5	Защита распределенных систем и	Стандарт X.509. Структура сертификата разных версий. Форматы хранения сертификатов
		Стандарт X.509. Принципы аутентификации. Отзыв сертификатов

	корпоративных сетей (ОПК-6)	Инфраструктуры открытых ключей
		Атакуемые сетевые компоненты информационных систем. Классификация нарушителей сетевой безопасности
		информационных систем
		Основные характеристики и типы брандмауэров и систем обнаружения и предотвращения вторжений
		Защищенный протокол передачи данных IPSec
		Защищенный протокол передачи данных SSL/TLS
6	Системы защиты электронной почты (ОПК-6)	Система защиты электронной почты PGP
		Система защиты электронной почты S/MIME
7	Организационное обеспечение информационной безопасности (ОПК-6)	Организационное обеспечение информационной безопасности

5.2.2. Перечень контрольных материалов для защиты курсового проекта/курсовой работы

Курсовые работы и курсовые проекты при изучении дисциплины не предусмотрены учебным планом.

5.3. Перечень индивидуальных домашних заданий, расчетно-графических заданий.

Расчетно-графические задания при изучении дисциплины не предусмотрены учебным планом.

5.4. Описание критериев оценивания компетенций и шкалы оценивания

При промежуточной аттестации в форме зачета используется следующая шкала оценивания: не зачтено, зачтено.

Компетенция ОПК-6. Способен использовать информацию, полученную при осуществлении своей профессиональной деятельности, с учетом основных требований информационной безопасности в том числе защиты государственной тайны.

ОПК-6.1 Использует информацию, полученную при осуществлении профессиональной деятельности с учетом требований информационной безопасности.

ОПК-6.2 Применяет методы информационной безопасности при подготовке проектной и технической документации в сфере профессиональной деятельности.

Критериями оценивания достижений показателей являются:

Наименование показателя оценивания результата обучения по дисциплине	Критерий оценивания
Знания	Технические и программные средств реализации информационных

	процессов; методы и процессы сбора, передачи, обработки и накопления информации.
	Теоретические основы изучаемых алгоритмов шифрования, формы защитыинформации в сети Интернет, требования к защите информации, критерии оценки угроз.
Умения	Использовать возможности вычислительной техники и программного обеспечения;
	Выполнять систематизацию технических данных;
	Осуществлять выбор наиболее эффективных методов,способов и средств получения, хранения и переработкиинформации в зависимости от конкретных целей и задачпрофессиональной деятельности;
	Проводить анализ необходимой информации, техниче- ских данных, показателей ирезультатов работы;
Навыки	Использовать возможности глобальных компьютерных сетей.
	Работать с различными источниками информации,используя разные формы защиты информации,выявлять программы – шпионы, «вирусы».

Оценка преподавателем выставляется интегрально с учётом всех показателей и критериев оценивания.

Оценка сформированности компетенций по показателю Знания.

Критерий	Уровень освоения и оценка	
	Не зачтено	зачтено
Знание терминов, определений, понятий	Не знает терминов и определений	Знает термины и определения, может корректно сформулировать их самостоятельно
Знание основных закономерностей, соотношений, принципов	Не знает основные закономерности и соотношения, принципы построения знаний	Знает основные закономерности, соотношения, принципы построения знаний, может самостоятельно их получить и использовать
Объем освоенного материала	Не знает значительной части материала дисциплины	Обладает твердым и полным знанием материала дисциплины, владеет дополнительными знаниями
Полнота ответов на вопросы	Не дает ответы на большинство вопросов	Дает полные, развернутые ответына поставленные вопросы
Четкость изложения и интерпретации знаний	Излагает знания без логической последовательности	Излагает знания в логической последовательности,самостоятельно их интерпретируя и анализируя

Оценка сформированности компетенций по показателю Умения.

Критерий	Уровень освоения и оценка	
	Не зачтено	Зачтено
Освоение методик - умение решать практические задачи, выполнять типовые задания	Не умеет решать практические задачи, выполнять типовые задания	Грамотно используетметодики, умеет решать все практические задачи, выполнять все типовые задания
Умение использовать теоретические знания для выбора методики решения задач, выполнения заданий	Не умеет использовать теоретические знания для выбораметодики решения задач, выполнениязаданий	Самостоятельно может сделать выбора методики решения задач, выполняет все задания без ошибок

Умение проверять решение и анализировать результаты	Не умеет проверять решение и анализировать результаты	Обладает твердыми умениями проверки решения и анализа результатов
Умение качественно оформлять (презентовать) решение задач и выполнения заданий	Не умеет качественно оформлять (презентовать) решение задач и выполнения заданий	Качественно и на высоком уровне оформляет решение задач и выполнения заданий

Оценка сформированности компетенций по показателю Навыки.

Критерий	Уровень освоения и оценка	
	Не зачтено	Зачтено
Навыки решения стандартных/нестандартных задач	Не может выполнять решения стандартных задач	Самостоятельно может выполнить решение стандартных/нестандартных задач
Объём выполненных заданий	Не выполняет значительную часть заданий по дисциплине	Выполняет весь объём заданий. Обладает твердым и полным знанием материала дисциплины, владеет дополнительными знаниями
Качество выполнения трудовых действий	Не выполняет трудовые действия	Обладает твердыми навыками выполнениятрудовых действий по всему материалу дисциплины, владеет дополнительными навыками
Самостоятельность планирования выполнения трудовых действий	Не выполняет планирования выполнения трудовых действий	Самостоятельно и грамотно выполняет планирование выполнения всех трудовых действий

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

6.1. Материально-техническое обеспечение

№	Наименование специальных помещений ипомещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1	Аудитория для лекционных занятий	Оборудованы специализированной мебелью, мобильным или стационарныммультимедийным проектором, переноснымэкраном, ноутбуком, или компьютером набазе одно или двухъядерных процессоров стактовой частотой не менее 2 ГГц, объемомоперативной памяти не менее 2 Гб и жесткого диска до 500 Гб; локальная сеть с пропускной способностью 100 Мбит/с
2	Компьютерные классы для проведениялабораторных занятий	Оборудованы специализированной мебелью, компьютерами с установленными программными продуктами на базе одно или двухъядерных процессоров с тактовой частотой не менее 2 ГГц, объемом оперативной памяти не менее 2 Гб и жесткого диска до 500 Гб; локальная сеть с пропускной способностью 100 Мбит/с, принтеры или многофункциональные устройства форматов А4, А3.
3	Помещения для самостоятельной работы обучающихся	Оборудованы специализированной мебелью, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации

6.2. Лицензионное и свободно распространяемое программное обеспечение

№	Перечень лицензионного программногообеспечения.	Реквизиты подтверждающего документа
1	Microsoft Office Professional Plus 2016	Соглашение Microsoft Open Value Subscription V6328633. Соглашение действительно с 02.10.2017 по 31.10.2023
2	Microsoft Windows 10 Корпоративная	Соглашение Microsoft Open Value Subscription V6328633. Соглашение действительно с 02.10.2017 по 31.10.2023). Договор поставки ПО 0326100004117000038-0003147-01 от 06.10.2017
3	Kaspersky Endpoint Security «Стандартный Russian Edition»	Сублицензионный договор № 102 от 24.05.2018.Срок действия лицензии до 19.08.2020 Гражданско-правовой Договор (Контракт) № 27782 «Поставка продления права пользования (лицензии) Kaspersky Endpoint Security от 03.06.2020. Срок действия лицензии 19.08.2023г.
4	Google Chrome	Свободно распространяемое ПО согласно условиям лицензионного соглашения
5	Mozilla Firefox	Свободно распространяемое ПО согласно условиям лицензионного соглашения
6	Microsoft Visual Studio 2013	договор №63-14кот 02.07.2014
7	Система компьютерного тестированиязнаний VeralTest (сетевая версия VeralSoft	электронное письмо от 06.04.2008

6.3. Перечень учебных изданий и учебно-методических материалов

1. Смышляев А. Г. Информационная безопасность и защита информации : метод. указания к выполнению лаб. работ / БГТУ им. В. Г. Шухова, каф. информ. технологий ; сост. А. Г. Смышляев. - Белгород : Изд-во БГТУ им. В. Г. Шухова, 2008. - 27 с.
2. Гашков, С. Б. Криптографические методы защиты информации : учеб. пособие / С. Б. Гашков, С. Б. Применко, М. А. Черепнев. - Москва : Академия, 2010. - 298 с.
3. Смышляев А. Г. Информационная безопасность : лаб. практикум : учеб. пособие / А. Г. Смышляев ; БГТУ им. В. Г. Шухова. - Белгород : Изд-во БГТУ им. В. Г. Шухова, 2015. - 101 с.
4. Лапонина, О. Р. Основы сетевой безопасности : криптографические алгоритмы и протоколы взаимодействия : учеб. пособие / О. Р. Лапонина. - 2-е изд., испр. . - Москва : Интернет-Университет Информационных Технологий ; Москва : БИНОМ. Лаборатория знаний, 2007. - 531 с.
5. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие / В. В. Платонов. - Москва : Академия, 2006. - 239 с

6.4.Перечень интернет ресурсов, профессиональных баз данных, информационно-справочных систем

1. Министерство науки и высшего образования РФ: http://minobrnauki.gov.ru
2. Российское образование ФЕДЕРАЛЬНЫЙ ПОРТАЛ: http://www.edu.ru
3. Сайт НТБ БГТУ им. В.Г. Шухова: http://ntb.bstu.ru
4. Электронно-библиотечная система «IPRBooks»: http://www.iprbookshop.ru
5. Электронная библиотечная система издательства «Лань»: http://e.lanbook.com
6. Научная электронная библиотека eLIBRARY.RU: http://elibrary.ru/
7. Электронно-библиотечная система «Университетская библиотека онлайн» (Библиоклуб.ру): http://biblioclub.ru/